

Amendments to the Claims:

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

1. (Currently Amended) A computer-implemented method for generating access control information, the method comprising:

receiving an access control rule that identifies a characteristic, the characteristic identifying an attribute from which attribute values of at least one user data entry and at least one object data entry are to be accessed and compared to generate access control information;

programmatically identifying at least one user data entry in user information that is associated with includes the attribute identified by the identified characteristic;

programmatically accessing, from the at least one user data entry, a first attribute value for the attribute identified by the identified characteristic and included in the at least one user data entry;

programmatically identifying at least one object data entry in data object information that is associated with includes the attribute identified by the identified characteristic; [[and]]

programmatically accessing, from the at least one object data entry, a second attribute value for the attribute identified by the identified characteristic and included in the at least one object data entry;

programmatically comparing the first attribute value with the second attribute value;

based on comparison results, programmatically determining whether the first attribute value corresponds to the second attribute value;

conditioned on determining that the first attribute value corresponds to the second attribute value, generating access control information that permits at least one user associated with the at least one user data entry in the user information to access the at least one object data entry in the data object information; and  
storing the generated access control information in electronic storage.

2. (Currently Amended) The method of claim 1 wherein:  
the identified characteristic is indirectly associated with the at least one user data entry in the user information, and  
programmatically identifying at least one user data entry in user information that is associated with includes the attribute identified by the identified characteristic comprises programmatically identifying at least one user data entry in user information that is indirectly associated with the identified characteristic.
3. (Currently Amended) The method of claim 1 wherein:  
the identified characteristic is directly associated with the at least one user data entry in the user information, and  
programmatically identifying at least one user data entry in user information that is associated with includes the attribute identified by the identified characteristic comprises programmatically identifying at least one user data entry in user information that is directly associated with the identified characteristic.

4. (Original) The method of claim 1 wherein generating access control information comprises:

generating user access control information that identifies the at least one entry in the user information that is associated with the identified characteristic,  
generating object access control information that identifies the at least one entry in the data object information that is associated with the identified characteristic, and

associating at least one entry in the user access control information with at least one entry in the data object access control information.

5. (Original) The method of claim 4 further comprising storing the association of the at least one entry in the user access control information with the at least one entry in the data object access control information.

6. (Original) The method of claim 4 further comprising:  
storing the data object access control information, and  
storing the user access control information.

7. (Original) The method of claim 4 further comprising determining whether a particular user associated with the at least one entry in the user access control information is permitted access to a particular data object that is associated with the at least one entry in the data object access control information wherein the determination is based on the association of the at least one entry in the user access control information with the at least one entry in the data object access control information.

8. (Original) The method of claim 1 further comprising receiving a filter condition, wherein generating access control information further comprises generating access control information by eliminating at least one entry in the user information that corresponds to the received filter condition such that access control information does not include the eliminated at least one entry in the user information.

9. (Original) The method of claim 1 further comprising receiving a filter condition, wherein generating access control information further comprises generating access control information by eliminating at least one entry in the data object information that corresponds to the received filter condition such that access control information does not include the eliminated at least one entry in the data object information.

10. (Currently Amended) A computer system for managing access control information for software operating on the computer system, the system comprising:

a data repository for access control information for software, the data repository including user information identifying a user characteristic for at least one entry in the user information, data object information identifying a data object characteristic for at least one entry in the data object information, and access control rule information identifying a shared characteristic for at least one entry in the access control rule information; and

an executable software module that causes (1) configured to:

programmatically identify at least one user data entry in user information that includes an attribute identified by the user characteristic;

programmatically access, from the at least one user data entry, a first attribute value for the attribute identified by the user characteristic and included in the at least one user data entry;

programmatically identify at least one object data entry in data object information that includes an attribute identified by the data object characteristic;

programmatically access, from the at least one object data entry, a second attribute value for the attribute identified by the data object characteristic and included in the at least one object data entry;

programmatically compare the first attribute value, the second attribute value, and an attribute value identified by the shared characteristic;

based on comparison results, programmatically determine whether the first attribute value corresponds to the second attribute value;

programmatic comparison of the user characteristic, the data object characteristic, and the shared characteristic and (2) generation of generate access control information for use in determining whether a user that is associated with [[an]] the at least one user data entry in the user information is permitted to access a data object that is associated with an the at least one object data entry in the data object information, generation of access control information comprises:

generating access control information that enables the user associated with the at least one user entry in the user information to access the at least one object data entry data object conditioned on determining that the first attribute value corresponds to the second attribute value programmatic comparison of the user characteristic, the data object characteristic and the shared characteristic indicating that the user characteristic corresponds to the shared characteristic and the data object characteristic corresponds to the shared characteristic, and

generating access control information that prevents the user associated with the at least one user entry in the user information from accessing the at least one object data entry data object conditioned on determining that the first attribute value does not correspond to the second attribute value; and programmatic comparison of the user characteristic, the data object characteristic and the shared characteristic indicating that the user characteristic does not correspond to the shared characteristic or the data object characteristic does not correspond to the shared characteristic

store the generated access control information in electronic storage.

11. (Original) The computer system of claim 10 further comprising a second executable software module that causes a determination whether a user associated with an entry in the user information is permitted to access a data object associated with an entry in the data object information such that the determination is based on the generated access control information.

12. (Original) The computer system of claim 11 wherein the second executable software module is the same executable software module as the first executable software module.

13. (Previously Presented) The computer system of claim 10 wherein the executable software module stores the generated access control information in electronic storage such that the generated access control rule information may be accessed to determine whether the user is permitted to access the data object when the user requests access to the data object subsequent to generation of the access control information.

14. (Original) The computer system of claim 10 wherein the executable software module causes an association between at least one entry in the user information and at least one entry in the access control information when the user characteristic corresponds to the shared characteristic.

15. (Original) The computer system of claim 14 wherein the executable software module causes an association between at least one entry in the data object information and at least one entry in the access control information when the data object characteristic corresponds to the shared characteristic.

16. (Original) The computer system of claim 15 wherein the executable software module causes a determination whether the user is permitted access to the data object based on the association of the user information to the shared characteristic and the association between the data object information and the shared characteristic.

17. (Original) The computer system of claim 10 wherein:  
the data repository includes:

user group information that associates a user group with at least one entry in the user information, and

access control rule information that identifies action that a user who is associated with group of users is permitted to perform on a data object, and

the executable software module causes a determination to be made, based on an association of the at least one entry in the user information with the user group, as to

whether the user associated with the at least one entry in the user information is permitted to perform a particular action on a particular data object.

18. (Currently Amended) A computer-readable medium having embodied thereon a computer program configured to generate access control information, the medium comprising one or more code segments configured to:

receive an access control rule that identifies a characteristic, the characteristic identifying an attribute from which attribute values of at least one user data entry and at least one object data entry are to be accessed and compared to generate access control information;

programmatically identify at least one user data entry in user information that is associated with includes the attribute identified by the identified characteristic;

programmatically access, from the at least one user data entry, a first attribute value for the attribute identified by the identified characteristic and included in the at least one user data entry;

programmatically identify at least one object data entry in data object information that is associated with includes the attribute identified by the identified characteristic; [[and]]

programmatically access, from the at least one object data entry, a second attribute value for the attribute identified by the identified characteristic and included in the at least one object data entry;

programmatically compare the first attribute value with the second attribute value; based on comparison results, programmatically determine whether the first attribute value corresponds to the second attribute value;

conditioned on determining that the first attribute value corresponds to the second attribute value, generate access control information that permits at least one user associated with the at least one user data entry in the user information to access the at least one object data entry in the data object information; and

store the generated access control information in electronic storage.

19. (Previously Presented) The medium of claim 18 wherein the one or more code segments configured to generate access control information comprise one or more code segments configured to:

generate user access control information that identifies the at least one entry in the user information that is associated with the identified characteristic,

generate object access control information that identifies the at least one entry in the data object information that is associated with the identified characteristic, and

associate at least one entry in the user access control information with at least one entry in the data object access control information.

20. (Previously Presented) The medium of claim 19 wherein the one or more code segments are further configured to determine whether a particular user associated with the at least one entry in the user access control information is permitted access to a particular data object that is associated with the at least one entry in the data object access control information wherein the determination is based on the association of the at least one entry in the user access control information with the at least one entry in the data object access control information.

21. (Previously Presented) The medium of claim 18 wherein the one or more code segments are further configured to:

receive a filter condition, and

generate access control information by eliminating at least one entry in the user information that corresponds to the received filter condition such that access control information does not include the eliminated at least one entry in the user information.

22. (Previously Presented) The medium of claim 18 wherein the one or more code segments are further configured to:

receive a filter condition, and

generate access control information further comprises generating access control information by eliminating at least one entry in the data object information that

corresponds to the received filter condition such that access control information does not include the eliminated at least one entry in the data object information.

23. (Currently Amended) The method of claim 1 wherein programmatically identifying at least one user data entry in user information that ~~is associated with~~ includes the attribute identified by the identified characteristic, programmatically identifying at least one object data entry in data object information that ~~is associated with~~ includes the attribute identified by the identified characteristic, and generating access control information that permits at least one user associated with the at least one user data entry in the user information to access the at least one object data entry in the data object. information occurs automatically without human intervention.

24. (Currently Amended) The method of claim 1 wherein:  
programmatically identifying at least one user data entry in user information that ~~is associated with~~ includes the attribute identified by the identified characteristic comprises:

programmatically identifying a first user data entry in user information that ~~is associated with~~ includes the attribute identified by the identified characteristic, and

programmatically identifying a second user data entry in user information that ~~is associated with~~ includes the attribute identified by the identified characteristic comprises, the first user data entry being associated with a first user and the second user data entry being associated with a second user that is different than the first user,

programmatically accessing, from the at least one user data entry, a first attribute value for the attribute identified by the identified characteristic and included in the at least one user data entry comprises:

programmatically accessing, from the first user data entry, a first attribute value for the attribute identified by the identified characteristic and included in the first user data entry, and

programmatically accessing, from the second user data entry, a third attribute value for the attribute identified by the identified characteristic and included in the second user data entry,

programmatically identifying at least one object data entry in data object information that is associated with includes the attribute identified by the identified characteristic comprises programmatically identifying a first data object in data object information that is associated with includes the attribute identified by the identified characteristic, [[and]]

programmatically accessing, from the at least one object data entry, a second attribute value for the attribute identified by the identified characteristic and included in the at least one object data entry comprises programmatically accessing, from the first data object, a second attribute value for the attribute identified by the identified characteristic and included in the first data object,

programmatically comparing the first attribute value with the second attribute value comprises programmatically comparing the first attribute value with the second attribute value and the third attribute value with the second attribute value,

based on comparison results, programmatically determining whether the first attribute value corresponds to the second attribute value comprises programmatically determining whether the first attribute value corresponds to the second attribute value and whether the third attribute value corresponds to the second attribute value,

conditioned on determining that the first attribute value corresponds to the second attribute value, generating access control information that permits at least one user associated with the at least one user data entry in the user information to access the at least one object data entry in the data object information comprises, conditioned on determining that the first attribute value corresponds to the second attribute value and the third attribute value corresponds to the second attribute value, generating first access control rule information that enables the first user to access the first data object and second access control rule information different than the first access control rule information that enables the second user to access the first data object.

25. (Previously Presented) The method of claim 24 further comprising:  
storing the generated access control information in electronic storage.

26. (Previously Presented) The method of claim 25 wherein storing the  
generated access control information in electronic storage comprises:

storing a first access control information data record that includes a first user  
identifier that identifies the first user and a first data object identifier that identifies the  
first data object, and

storing a second access control information data record that includes a second  
user identifier that identifies the second user and a second data object identifier that  
identifies the first data object.